חישוביות - שיעור 9

דוד קלוטה

31 במאי 2026

בשיעור הקודם

השתמשנו במשפט קוק־לוין לצורך מספר הוכחות, אך עדיין לא ניסחנו והוכחנו אותו.

התחלנו!

9.1 משפט קוק־לוין

משפט 9.1.1. *מתקיים כי השפה* $\mathrm{CNF-SAT}$ *היא* NP*־שלמה.*

נזכור:

$$\mathrm{CNF-SAT} \overset{\text{def}}{=\!=} \{\phi \mid \phi \textit{ is a satisfiable CNF formula}\}$$

כאשר נוסחת CNF *היא מבנה של פסוקיות. בתוך כל פסוקית נמצאים ליטרלים (משתנים ושלילת משתנים) וביניהם הסימן* $\vee$*. בין הפסוקיות יהיה הסימן* $\wedge$*.*

אם הנוסחה ϕ *ספיקה, אזי קיימת הצבה למשתנים אשר נותנת ערך* True *ל־*ϕ*.*

הוכחה. הראינו ש־$\mathrm{CNF-SAT} \in \mathrm{NP}$. נותר להראות ששפה זו היא NP־קשה.

כלומר, להראות שלכל $L \in \mathrm{NP}$ מתקיים $L \leqslant_{\mathrm{P}} \mathrm{CNF-SAT}$. זה אומר שלכל $L \in \mathrm{NP}$ קיימת פונקציה החשיבה בזמן פולינומי f כך ש־

$$\forall w \in \Sigma^* : \quad w \in L \iff f(w) \in \mathrm{CNF-SAT}$$

הנחתנו היחידה על L זה כי היא שייכת ל־NP. כלומר, יש מכונת טיורינג לא דטרמיניסטית פולינומית M המכריעה את L.

נרצה לכל מילה $w \in \Sigma^*$ (המועמדת לשייכות ל־L לייצר נוסחה ϕ בזמן פולינומי כך ש:

1. ϕ נוסחת CNF
2. ϕ ספיקה אמ"ם $w \in L$.

רעיון ההוכחה יהיה כך ש־ϕ תדמה ריצה $M(w)$. תהיה הצבה מספקת ל־ϕ אמ"ם תהיה ריצה מקבלת של $M(w)$.

נתאר טבלה עבור ריצה של M על w - שורה לכל קונפיגורציה (קונפיגורציה היא תיאור של המכונה [מצב, מיקום, ראש, תוכן סרט].

פורמלית, $c = uqv$ כאשר $q \in Q$ ו־$u, v \in \Gamma^*$. לדוגמה, הקונפיגורציה ההתחלתית אם הקלט $w \in \Sigma^*$ היא $c_0 = q_0 w$):

טבלה 1: הטבלה הרלוונטית

c_0					
c_1					
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
c_i					
c_{i+1}					
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
c_m					

גובה הטבלה יהיה m כמספר צעדי הריצה.

הערה **9.1.1.** n פולינומי ב־$|w|$.

רוחב הטבלה, בה"כ m, כי בזמן m ניתן לכתוב לכל היותר ב־m תאים.

הרעיון:

1. נתאר אוסף של בדיקות שמוודא שמילוי הטבלה מתאים לרייצה חוקית שמתחילה מהקונפיגורציה ההתחלתית ומסתיימת בקונפיגורציה מקבלת, וכל שתי שורות עוקבות מתאימות למעבר חוקי של δ. כל תא בטבלה הוא אות מתוך $Q \cup \Gamma$.

2. נראה איך להמיר את אוסף הבדיקות הללו לנוסחת CNF מעל משתנים בוליאנים.

טענת עזר 9.1.1. *בה"כ, לכל אורך קלט יש קונפיגורציה מקבלת יחידה.*

הוכחה. בהינתן מכונת NP M עבור L, נוכל לשנות אותה באופן הבא: את מצב q_{acc} נשנה למצב $q_{\text{almost accept}}$. במצב זה: המכונה תמחק את כל הסרט, תחזיר את הראש לתחילת הסרט ואז תעבור למצב q_{acc}. ברור שהמכונה החדשה מחזירה אותן תשובות q_{acc} או q_{rej} כמו המקורית. זמן הריצה נשאר פולינומי, אבל עכשיו יש קונפיגורציה מקבלת יחידה $c_m = q_{\text{acc}}$. □

איך נבדוק אם c_i, c_{i+1} (שורות בטבלה) מתאימות לקונפיגורציות עוקבות אחת אחרי השנייה? נשים לב שזוג גונפיגורציות עוקבות הן זהות כמעט בכל מקום למעט במקום בו נמצא הראש, שם ייתכן שינוי מצב, כתיבת אות ותנועה ימינה / שמאלה - כל זה בהתאם לפונקצייה δ. נסתכל על שישיית תאים בטבלה של שלשה בשורה c_i ושלשה מתאימה בשורה c_{i+1}. איזה מילוי הוא חוקי עבור השישייה?

1. העתקה (אין ראש באזור): $\forall \alpha, \beta, \gamma \in \Gamma$, הטבלה תיראה כך:

טבלה 2: השישייה בסעיף 1

α	β	γ
α	β	γ

2. על כל מעבר חוקי של פונקצייה δ: $(q_2, \beta, R) \in \delta(q_1, \alpha)$ הטבלה תיראה כך:

טבלה 3: סטטוס הטבלה בסעיף 2 לימין

	η	ζ	q_1	α	γ	δ
	η	ζ	β	q_2	γ	δ

בעצם, לכל מעבר חוקי $(q_2, \beta, R) \in \delta(q_1, \alpha)$ ולכל $\gamma, \delta, \zeta, \eta \in \Gamma$ נרצה לאשר כל אחד מהמילויים הבאים לשישייה:

q_1	α	γ
β	q_2	γ

ζ	q_1	α
ζ	β	q_2

η	ζ	q_1	α
η	ζ	β	q_2

q_1	α	γ	δ
β	q_2	γ	δ

איור 1: השישיות האפשריות

באופן דומה עבור תנועה שמאלה $(q_2, \beta, L) \in \delta(q_1, \alpha)$ הטבלה תיארה כך:

טבלה 4: סטטוס הטבלה בסעיף 2 לשמאל

η	ζ	q_1	α	γ	δ	
η	q_2	ζ	β	γ	δ	

בעצם, לכל מעבר חוקי $(q_2, \beta, L) \in \delta(q_1, a)$ ולכל $\gamma, \delta, \zeta, \eta, \iota \in \Gamma$ נרצה לאשר כל אחד מהמילויים הבאים לשישייה:

ζ	q_1	α	γ
q_2	ζ	β	γ

ζ	q_1	α
q_2	ζ	β

η	ζ	q_1	α
η	q_2	ζ	β

ι	η	ζ	q_1	α
ι	η	q_2	ζ	α

ζ	q_1	α	γ	δ
q_2	ζ	β	γ	δ

איור 2: השישיות האפשריות

נרצה להחליף את תאי הטבלה במשתנים בוליאנים (כמה משתנים לכל תא בטבלה) ואת הבדיקות שתיארנו עד כה, לנוסחאות בוליאניות מעל המשתנים הנ"ל בתצורת CNF.

תהי נוסחת CNF q_{init} שתבדוק נכונות שורה c_0. תהי נוסחת CNF q_m שתבדוק נכונות שורה c_m ולכל $i,j \in [m-1] \cup \{0\}$ נחסות ϕ^{ij}_{move} שבודקת האם השישייה שהפינה השמאלית עליונה בקואואדינטות i,j קיבתה מילוי חוקי וגם היא תהיה מתצורת $(m-1)$CNF.

נגדיר את ϕ להיות:

$$\phi = \phi_{\text{init}} \wedge \phi_m \wedge \bigwedge_{i,j=0}^{m-1} \phi^{ik}_{\text{move}}$$

ונקבל נוסחת CNF שתהיה ספיקה אמ"ם מתאימה למילוי חוקי של הטבלה, כלומר אמ"ם יש ריצה מקבלת של M מעל w.

איך נעבור מהטבלה לנוסחת CNF? נסתכל על בדיקה של שישייה אחת. זוהי בדיקה של 6 משתנים בתחום $Q \cup \Gamma$.

כל תא בטבלה הוא משתנה שמקבל ערך בתחום $Q \cup \Gamma$. בשישייה יש 6 משתנים כאלה, ביחד מקבלים ערך מתוך $(Q \cup \Gamma)^6$. אפשר לקודד כל תא ב־$t \overset{\text{def}}{=\!=} \lceil \log_2 |Q \cup \Gamma| \rceil$ משתנים בוליאנים. נרשום טבלה שמתארת את כל ההצבות החוקיות לשישייה - ונקבל גם את ההצבות החוקיות ל־$6t$ המשתנים הבוליאניים. קל להפוך את הטבלה הזו לנוסחת DNF שבודקת חוקיות הצבה למשתנים הבוליאניים. כלומר, הנוסחה תהיה $\vee$ של פסוקיות: כל פסוקית מתאימה לשורה אחת בטבלה, כלומר הצבה אחת ל־$6t$ המשתנים הבוליאניים. הפסוקית תהיה רצף של $\wedge$ שמאלץ את הערכים הבינאריים ל־$6t$ המשתנים.

טבלה 5: השינוי

l_1	l_2	l_3	l_4	l_5	l_6	x_1	x_2	x_3	x_4	$\dots$	x_{6t}
α	q_1	γ	η	α	β	0	1	0	0	$\dots$	

בעצם -

$$\begin{aligned} &(\overline{x_1} \wedge x_2 \wedge \overline{x_3} \wedge \overline{x_4} \dots) \\ \vee &(\dots) \\ \vee &(\dots) \end{aligned}$$

כדי לקבל נוסחת CNF שמבצעת את אותה הבדיקה, ניצור נוסחת DNF עבור הפונקציה המשלימה. כלומר טבלה כנ"ל עם כל הערכים האסורים לשישייה. ניקח שלילה של הנוסחה המתקבלת: כל $\wedge$ הופך ל־$\vee$ - כל $\vee$ הופך ל־$\wedge$, הליטרל x הופך ל־$\overline{x}$ והליטרל $\overline{y}$ הופך ל־y. קיבלנו נוסחת CNF שבודקת נכונות של שישייה אחת: הנוסחאות ϕ^{ij}_{move} השונות (עבור ערכי i,j שונים) נראות כמעט זהות - כל ההבדל הוא בשמות המשתנים לפי i,j.

נרצה לסגור את הוכחת קוק לוין, כלומר להשתכנע שלכל $L \in \text{NP}$ מתקיים $L \leqslant_{\text{P}} \text{CNF}-\text{SAT}$. משום ש־$L \in \text{NP}$, קיימת מכונת טיורינג לא דטרמיניסטית M עבור L. בהינתן $w \in \Sigma^*$ נרצה בזמן פולינומי ב־$|w|$ לייצר נוסחה ϕ מתצורת CNF כך ש־

$$w \in L \iff \phi \in \text{CNF}-\text{SAT}$$

בנייה בהינתן w נייצר את $\phi_{\text{init}}, \phi_m, \phi^{ij}_{\text{move}}$ באופן שתיארנו דלעיל כך ש־m חסם על זמן הריצה $M(w)$. נחזיר ϕ שהיא $\wedge$ על כל הבדיקות הנ"ל. ברור שניתן לייצר את הכל בזמן פולינומי ב־$|w|$. נשים לב שייצור ϕ^{ij}_{move} דורש מונים כדי לעקוב אחרי ערכי i,j אבל מבנה הנוסחה לא משתנה.

נכונות אם $w \in L$ אז קיימת ריצה מקבלת של $M(w)$. לכן קיים מילוי חוקי לטבלת הקונפיגורציות (כבל תא ערך מתוך $Q \cup \Gamma$) שמתאים לריצה מקבלץ לרכן הקידוד הבינארי של המילוי הנ"ל ייתן ערך True לכל אחת מהבדיקות, כלומר יש הצבה מספקת ל־ϕ. ואם $w \notin L$ אז אין ריצה מקבלת של $M(w)$. לכן כל מילוי של הטבלה אינו חוקי, כלומר שורה c_0 אינה קונפיגורציה התחלתית או שורה c_m אינה קונפיגורציה מקבלת או שיש זוג שורות עוקבות c_i, c_{i+1} שאינן קונפיגורציות עוקבות ולכן לפחות אחת מהבדיקות תיכשל. כלומר לפחות פסוקית אחת בלפחות נוסחה בוליאנית אחת שמרכיבה את ϕ תקבל False, כלומר ϕ איננה ספיקה, ולכן לא ב־$\mathrm{CNF-SAT}$. □

זו הייתה ההוכחה הארוכה ביותר שנראתה בקורס - על אף שאף אחד מהשלבים שלא לא קשה מדי בעצמו. ככל הנראה לא הבנתם אותה בפעם הראשונה - במקום זאת, עליכם לקרוא ולהסביר.

9.2 בעיית $\mathrm{SUBSET-SUM}$

הגדרה 9.2.1. בעיית $\mathrm{SUBSET-SUM}$ היא

$$\mathrm{SUBSET-SUM} \stackrel{\text{def}}{=} \left\{ (s, a_1, a_2, \ldots, a_n) \;\middle|\; \begin{array}{l} s \in \mathbb{Z},\ a_i \in \mathbb{Z} \text{ for each } i \in \mathbb{N}, \\ \text{there exists a subset } I \subseteq \{a_i\}_{i\in[n]} \\ \text{such that } \sum_{x\in I} x = s \end{array} \right\}$$

טענה 9.2.1. *מתקיים כי* $\mathrm{SUBSET-SUM}$ *היא* NP־*שלמה.*

הוכחה. נוכיח את שתי טענות העזר הבאות, וההוכחה שלנו תסתיים:

טענת עזר 9.2.1. *מתקיים כי* $\mathrm{SUBSET-SUM} \in \mathrm{NP}$.

הוכחה. נראה מוודא פולינומי:

Algorithm 1 Polynomial verifier for $\mathrm{SUBSET-SUM}$

Require: $s \in \mathbb{Z}$
Require: $(a_i)_{i\in[n]} \subseteq \mathbb{Z}$
Require: C is a subset of S
1: **return** $\sum_{x\in C} x = s$

נכונות וזמן ריצה ברורים. □

טענת עזר 9.2.2. *מתקיים כי* $\mathrm{SUBSET-SUM}$ *היא* NP־*קשה.*

הוכחה. נוכיח כי $3\mathrm{SAT} \leqslant_{\mathrm{P}} \mathrm{SUBSET-SUM}$, כלומר נגדיר $\phi \overset{P}{\mapsto} (S, a_1, \ldots, a_n)$ כך ש־

$$\phi \in 3\mathrm{SAT} \iff (S, a_1, \ldots, a_n) \in \mathrm{SUBSET-SUM}$$

וכיוון שהראינו כי $3\mathrm{SAT}$ היא NP־קשה, נסיק מטרנזיטיביות כי גם $\mathrm{SUBSET-SUM}$.

בנייה בעבור ϕ, נעביר שורה בבלה לכל משתנה ושלילתו, עמודות לכל אחד מהפסוקיות. כל שורה תתאים למספר ארוך, ותהיה שורה נוספת עבור S.

ב־ϕ יש משתנים ו־m פסוקיות. נסמן ספרה 1 בכל מפגש של עמודת פסוקית עם שורת ליטרל, אמ"ם הליטרל מופיע בפסוקית. 0 אחרת. ברור שהבנייה פולינומיאלית. נותר להוכיח נכונות:

נכונות נניח כי ϕ ספיקה. נסתכל על הצבה מספקת, ונבחר את המספרים שמתאימים לשורות של הליטרלים שקיבלו True. בנוסף, מ־$2m$ השורות התחתונות נשלים לפי הצורך. נשים לב שבכל עמודה מ־n הראשונות יש בדיוק 1 אחד שנבחר. לכן סכום בכל עמודה כזו בדיוק 1. בנוסף, בכל עמודה מ־m האחרונות, הסכום מ־$2n$ השורות הראשונות הוא לפחות אחד בכל עמודה - כי בכל פסוקית יש לפחות ליטרל אחד שקיבל True. לכן יש דרך להשלים שורות מ־$2m$ התחתונות כך שהסכום בכל עמודה יהיה בדיוק 3. נניח כעת כי יש תת־קבוצה של מספרים (שורות) שסכומן בדיוק s, אז מכל זוג של משתנה ושלילתו בדיוק שורה אחת נבחרה, כי סכום ב־n העמודות הראשונות הוא 1 בכל עמודה. נפרש את הבחירה הזו כהצבה ל־ϕ. כלומר, $x_i = \mathrm{True}$ אמ"ם השורה של x_i נבחרה. וגם $x_i = \mathrm{False}$ אם השורה של $\overline{x_i}$ נבחרה. $2m$ השורות התחתונות יכולות לתרום לכל היותר 2 לכל עמודה מ־m העמודות הימניות של הפסוקיות, אבל הסכום הוא 3 בכל עמודה כזו. מכאן שלכל עמודה יש לפחות שורה אחת מ־$2n$ הראשונות שתורמת לה 1. זה אומר שלכל פסוקית יש ליטרל שקיבל True ומכאן ϕ ספיקה. □

הערה 9.2.1. צריך בסיס מספיק גדול בשביל שלא יהיה carry.

עם שתי טענות עזר אלה, מהגדרת NP־שלמות סיימנו. □